METHOD AND ARRANGEMENT FOR FORMING A SECRET COMMUNICATION KEY FOR A PREDETERMINED ASYMMETRIC CRYPTOGRAPHIC KEY PAIR

The invention relates to a method and an arrangement for forming a secret communication key for a predetermined asymmetric key pair.

The formation of an asymmetric cryptographic key pair is known from [1].

Given this method, the RSA method for forming a cryptographic key pair, which comprises a secret key and a corresponding public key, is formed.

Only the user knows the secret key; the public key can be made known to all subscribers of a communication network.

The user signs the data with his secret key when a digital signature is prepared for protecting the authenticity and integrity of electronic data. The signed digital signature is verified upon utilization of the public key corresponding to the secret key, so that the authenticity or, respectively, integrity of the digital signature can be checked by all communication partners, which have access to the public key.

The aforementioned what is referred to as "Public-Key-Technology" is particularly applied in the digital communication within a computer network (a fixed number of computer units, which are connected to one another via a communication network).

Given the method known from [1], the protection of the secret key against unauthorized access of a third party is of critical importance for the security of the digital signature.

It is known from [2] to store the secret key on an external medium for storing data, for example a chip card, a disk etc., or on a hard disk, whereby key data are protected in that a personal identification code (Personal Identification Number, PIN) or a password, with which the key data are respectively deciphered is used. It is necessary, however, to access the local resources of a user when these external media are used. This is not desired especially with respect to a network-oriented infrastructure of network computers or Java applications.

A network computer is a computer, which is networked with other computers.

A Java application is a program containing programs that are written in the programming language Java.

Therefore, the method known from [2] is associated with the disadvantage that the secret key must be stored on an external medium, so that it is very difficult to protect the secret key against misuse.

An overview regarding hash functions can be found in [3]. A hash function is a function, wherein it is possible to calculate a corresponding input value to a given function value. Furthermore, an output character string having a fixed length is allocated to an arbitrarily long input character string. Moreover, additional properties can be requested for the hash function. Such an additional property is collision freedom, i.e., it is not allowed to be possible to find two different input character strings resulting in the same output character string.

Examples of a hash function are the method according to the MD-2 standard, the method according to the MD-5 standard, the Data Encryption Standard (DES), which is carried out without utilizing a key, or any other arbitrary hash function.

A method referred to as a method according to Miller-Rabin, wherein it can be checked for a number whether it is a prime number, is known from [4].

Therefore, an object of the invention is to form a secret communication key for a predetermined asymmetric cryptographic key pair, wherein the secret key of the asymmetric key pair must not be stored permanently.

The problem is solved by the method and by the arrangement with the features of the independent patent claims.

Given the method for forming a secret communication key for a predetermined asymmetric cryptographic key pair, which comprises a secret key and a corresponding public key, a prescribable initial value has been used with respect to the determination of the key pair. The initial value is available to a user. The user enters the initial value into the computer and the secret communication key is formed upon utilization of the initial value. The secret communication key and the public key form a communication key pair.

The arrangement for forming a secret communication key for a predetermined asymmetric cryptographic key pair, which comprises a secret key and a corresponding public key, has a processor, which is set up such that the following steps can be carried out:

- a prescribed initial value has been used for determining the key pair,
- the user enters the initial value into the computer,
- the secret communication key is formed upon utilization of the initial value, whereby the secret communication key and the public key form a communication key pair.

Furthermore, an input means is provided for entering the initial value by the user.

As a result of the invention, it is possible to erase the secret key without having to forego the intense cryptography of the "Public-Key-Technology".

Concretely, the initial value can be regarded as a personal identification code (Personal Identification Number PIN) or as a password that is prescribed by the user or that is centrally prescribed and that is entered by the user into the computer. After the password or, respectively, the PIN has been entered, the secret communication key, i.e. the key that is of the same name compared to the secret key, is formed, which forms a key pair, the communication key pair, together with the public key, upon utilization of the the [sic] password or, respectively, of the PIN as an initial value. [sic]

In this way, a fusion of the password technology customary to the user of a conventional computer network or, respectively, of a conventional computer with the intense cryptology is inventively achieved without considerable efforts being necessary in order to permanently store secret key material.

Preferred embodiments of the invention derive from the dependent claims.

In an embodiment of the invention, a hash function is applied to the initial value, whereby a value is formed that is finally used for the key generation.

Furthermore, additional data, which preferably characterize the user himself, can be used during the key generation.

The RSA method for the key generation is preferably used for forming the cryptographic key.

The method according to the MD-5 standard, the MD-2 standard or the Data Encryption Standard (DES) can be used as hash function can be used [sic].

The communication key pair can be used for enciphering or for securing the integrity of electronic data, for forming a digital signature via electronic data or for

authenticating a user, generally for any arbitrary cryptographic operation using the "Public-Key-Technology", whereby the formed communication key pair is utilized.

For accelerating the method, it is advantageous in an embodiment to store an index when the secrete key is formed, which index is referred to as accelerating code in the following. The accelerating code indicates how often numbers - proceeding from the initial value - have been checked to the effect whether or not the respective number is a prime number.

The method according to Miller-Rabin is preferably used for checking the property whether a number represents a prime number.

An exemplary embodiment of the invention is shown in the Figures and is subsequently explained in greater detail.

Shown are

Figure 1 a flow diagram representing the method steps of the exemplary embodiment;

Figure 2 a drawing representing a computer network having a plurality of computers coupled to one another;

Figure 3 a symbolic drawing representing the course of action for determining a prime number on the basis of an initial value.

Figure 2 shows a plurality of computers 200, 210, 220, 230, 240, 250, which are connected to one another via a communication network 260. Each computer 200, 210, 220, 230, 240, 250 respectively has a plurality of input means, i.e. a keyboard 206, 216, 226, 236, 246, 256, a mouse 207, 217, 227, 237, 247, 257, a scanner (not

shown) or a camera (not shown). The entered information is supplied to a memory 202, 212, 222, 232, 242, 252 via the respective input means via an input interface/output interface 201, 211, 221, 231, 241, 251 and is stored. The 202, 2212, 222, 232, 242, 252 memory is connected to the input interface/output interface 201, 211, 221, 231, 241, 251 via a bus 204, 214, 224, 234, 254. A processor 203, 213, 223, 233, 243, 253, which is set up such that the following methods steps can be carried out, is also connected to the bus 204, 214, 224, 234, 254.

The computer 200, 210, 220, 230, 240, 250 communicate via the communication network 260 according to the Transport Control Protocol/Internet Protocol (TCP/IP).

The communication network 260 also contains a certification unit 270 with which a certificate is prepared respectively for a public key, so that the public key is trustworthy for a communication on the basis of the "Public-Key-Technology".

A user 280 enters an arbitrary prescribable word (PIN, password), which is only known to the user, into a first computer 200 (step 101, compare **Figure 1**).

According to the RSA method, the first computer 200 generates an asymmetric cryptographic key pair, as described in the following.

The value 102 entered by the user 280 and additional data 103 characterizing the user 280, such as user name, personal number, terminal address etc., are supplied to a hash function (step 104).

[3] contains an overview regarding hash functions. A hash function is a function, wherein it is not possible to calculate a corresponding input value to a given function value. Furthermore, an output character string having a fixed length is allocated to an arbitrarily long input character string. Moreover, additional properties can be requested for the hash function. Such an additional property is collision freedom, i.e.,

it is not allowed to be possible to find two different input character strings resulting in the same output character string.

Examples of a hash function are the method according to the MD-2 standard, the method according to the MD-5 standard, the Data Encryption Standard (DES), which is carried out without utilizing a key, or any other arbitrary hash function.

The value formed by the hash function is used as base value BW for forming two prime numbers, as symbolically shown in **Figure 3.**

As shown in **Figure 3**, it is respectively checked for a value Wi (i = 1, ..., n) in an iterative method, on the basis of the base value BW, whether or not the respective value represents a prime number (step 301).

The method according to Miller-Rabin is utilized as method for checking the property prime for a number (see [4]).

If it is determined for a number that the number does not represent a prime number, the number is increased by a prescribable value, preferably by the value 2 (step 302) and the test with respect to the property "prime" is repeated (step 301). This course of action is repeated until two prime numbers - a first prime number P and a second prime number q - have been determined.

Referred to as index is a number indicating how often - on the basis of the base value PW [sic] - the number must be increased by the prescribed value until the first prime number p or, respectively, the second prime number q is obtained.

The result of the method shown in **Figure 3** is two prime numbers p and q, which are used for the key generation according to the RSA method (step 105).

The prime numbers p and q normally have a length of a plurality of 100 bit.

A modulus n is formed from the prime numbers p and q according to the following rule:

$$n = p * q. \quad (1)$$

Furthermore, an intermediate variable $\varphi(n)$ is formed according to the following rule:

$$\varphi(n) = (p-1) * (q-1). \quad (2)$$

A secret key d is now selected such that the secret key d is relatively prime with respect to φ (n). A public key e is determined such that the following rule is fulfilled:

$$e * d \text{ mop } \varphi(n) = 1. \quad (3)$$

The value d is the secret key and is not allowed to make known to a third party.

Therefore, a private key d (step 106) and a public key e (step 107) have been formed as a result of the key generation (key 105).

The two keys d, e form a cryptographic key pair corresponding to one another, this key pair being used for an arbitrary cryptographic operation, i.e. for enciphering, deciphering, for the digital signature or for authenticating (step 108).

After the key pair d, e has been formed according to the above-described method, the secret key d is erased.

The public key e is supplied to the certification entity 280. A certificate Certe is formed by the certification entity 280 via the public key e and the certificate Certe of the public key e is stored in a directory 290 that can be accessed by the public.

Therefore, each communication participant in the communication network 280 can access the public key e via the certificate Certe of the public key e.

The secrete key d corresponding to the public key e is erased in the first computer 200.

Every time when the user 280 wishes to initial a communication on the basis of the key pair or, respectively, when the user 280 wishes to carry out a cryptographic operation upon utilization of such a key pair, the user 208 [sic] enters his initial value (PIN, password) into the first computer 200 and the initial value 102 (as described above), in turn, is provided with additional data 103, is subjected to a hash function (step 104) and, on the basis of the base value BW, two prime numbers p and q are determined or a stored index (as described above) is read out or is also entered by the user 280 and a secrete communication key is formed therefrom, which, however, corresponds to the secrete, previously formed key d, which has been erased again.

In this way, a communication key pair has been formed, which comprises the secrete communication key and the corresponding public key e. For a communication session, a user can thus respectively currently generate the secrete communication code, so that it is possible to use intense "Public-Key-Technology" without having to store the secrete key on a chip card.

The thus generated communication key pair d, e is used for enciphering plaintext 109 with the public key e and for deciphering the electronic, enciphered data 110 with the secrete communication key.

Figure 1 symbolically shows the processing of plaintext 109, i.e., electronic data 109 that can be read by everybody, as well as enciphered electronic data 110, whereby the communication device respectively describes by an arrow toward or, respectively, from the block representing a cryptographic operation 108. [sic]

The enciphering or, respectively, deciphering is performed according to the following rules:

$$m^e \bmod n = c, \qquad (4)$$

whereby

- m refers to a quantity of 512 bit of electronic data 109 to be enciphered,
- c refers to enciphered electronic data 110.

The deciphering of the enciphered electronic data c is performed according to the following rule:

$$m = c^d \bmod n. \qquad (5)$$

A few alternatives of the above-described exemplary embodiment are explained in the following:

The method can be used for enciphering, for securing integrity and for the digital signature of electronic data.

Furthermore, the invention can be utilized in the field of secure electronic mail systems.

The user must not necessarily enter the initial value 102 during the generation of the key pair at the beginning of the method, but a central unit generating the key pair can prescribe it to the user.

Therefore, the user must merely remember a password or, respectively, a PIN and it is no longer necessary to securely store a secrete cryptographic key, for example on a chip card, this being associated with corresponding risks and with considerable outlay.

Instead of a hash function, any arbitrary one-way function can be used in the framework of the invention.

The following publications have been cited in the framework of this document.

[1] C. Ruland, Informationssicherheit in Datennetzen, ISBN 3-89238-081-3, DATACOM-Verlag, page 79 - 85, 1993

[2] D. Longley and M. Shain, Data & Computer Security, Dictionary of standards concepts and terms, Stockton Press, ISBN 0-333-42935-4, page 317, 1987

[3] [1] C. Ruland, Informationssicherheit in Datennetzen, ISBN 3-89238-081-3, DATACOM-Verlag, page 68 - 73, 1993

[4] A. J. Menezes, P. van Oorschot and S. Vanstone, Handbook of Applied Cryptography, CRC Press, ISBN 0-8493-8523-7, page 138 - 140, 1997